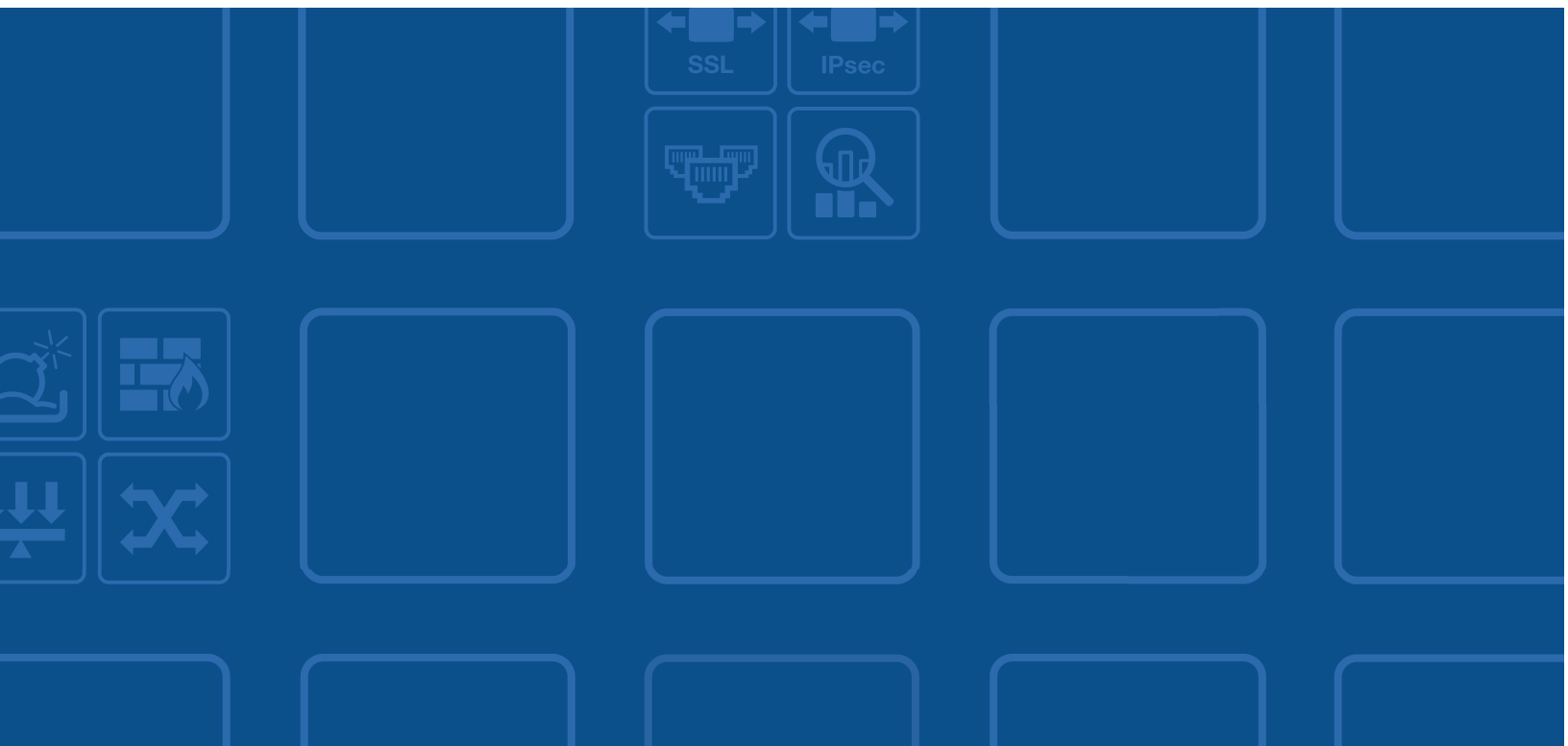
FORTINET
High Performance Network Security

FortiOS - Release Notes

VERSION 5.4.6



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

January 12, 2018

FortiOS 5.4.6 Release Notes

01-546-446948-20180112

TABLE OF CONTENTS

Change Log **5**
Introduction **6**
Supported models 6
Special branch supported models 7
What's new in FortiOS 5.4.6 8
Special Notices **9**
Built-In Certificate 9
Default log setting change 9
Policy list display changes 9
FortiAnalyzer support 9
Removed SSL/HTTPS/SMTPS/IMAPS/POP3S 10
FortiGate and FortiWiFi-92D hardware limitation 10
FG-900D and FG-1000D 10
FG-3700DX 10
FortiGate units managed by FortiManager 5.0 or 5.2 11
FortiClient support 11
FortiClient (Mac OS X) SSL VPN requirements 11
FortiGate-VM 5.4 for VMware ESXi 11
FortiClient profile changes 11
FortiPresence 12
Log disk usage 12
SSL VPN setting page 12
FG-30E-3G4G and FWF-30E-3G4G MODEM firmware upgrade 12
Use of dedicated management interfaces (mgmt1 and mgmt2) 13
DLP, AV 13
Using ssh-dss algorithm to log in to FortiGate 13
Upgrade Information **14**
Upgrading to FortiOS 5.4.6 14
Upgrading to FortiOS 5.6.0 14
Cooperative Security Fabric upgrade 14
FortiGate-VM 5.4 for VMware ESXi 15
Downgrading to previous firmware versions 15
Amazon AWS enhanced networking compatibility issue 15
FortiGate VM firmware 16

Firmware image checksums 16
Product Integration and Support **17**
FortiOS 5.4.6 support 17
Language support 20
SSL VPN support 20
SSL VPN standalone client 20
SSL VPN web mode 21
SSL VPN host compatibility list 21
Resolved Issues **23**
Known Issues **32**
Limitations **37**
Citrix XenServer limitations 37
Open Source XenServer limitations 37

Change Log

Date	Change Description
2017-10-19	Initial release of FortiOS 5.4.6.
2017-10-20	Moved 398397 and 403146 from *Known Issues* to *Resolved Issues*. In *Resolved Issues* section: • Updated 417001 and 420967. • Added 390495, 412404, and 423819.
2017-10-26	Clarified note in *Upgrading to FortiOS 5.6.0*. Added *Special Notices* > *Policy list display changes* section. Added 435095 to *Resolved Issues*. Added 456566 to *Known Issues*.
2017-11-06	Updated 422133 in *Resolved Issues* > *Common Vulnerabilities and Exposures*.
2017-11-10	Added 273973 to *Resolved Issues*. Added 421423 to *Known Issues*.
2017-11-10	Added 436126 to *Resolved Issues*.
2017-11-28	Added 401360 to *Resolved Issues*.
2017-12-18	Moved 374521 from *Known Issues* to *Resolved Issues*. Added 415353 to *Resolved Issues*.
2018-01-09	Deleted 299490 from *Known Issues*. Moved 364280 to *Special Notices* > *Using ssh-dss algorithm to log in to FortiGate*.
2018-01-12	Added 445174 to *Resolved Issues*.

Introduction

This document provides the following information for FortiOS 5.4.6 build 1165:

- Special Notices
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues
- Limitations

See the Fortinet Document Library for FortiOS documentation.

Supported models

FortiOS 5.4.6 supports the following models.

FortiGate	FG-30D, FG-30E, FG-30D-POE, FG-50E, FG-51E, FG-60D, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-140D, FG-140D-POE, FG- 200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300D, FG-400D, FG-500D, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3800D, FG-3810D, FG-3815D, FG-5001C, FG-5001D
FortiWiFi	FWF-30D, FWF-30E, FWF-30D-POE, FWF-50E, FWF-51E, FWF-60D, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE
FortiGate Rugged	FGR-60D, FGR-90D
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VMX, FG-VM64-XEN FortiOS 5.4.6 supports the additional CPU cores through a license update on the following VM models: • VMware 16, 32, unlimited • KVM 16 • Hyper-V 16, 32, unlimited
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM
FortiOS Carrier	FortiOS Carrier 5.4.6 images are delivered upon request and are not available on the customer support firmware download page.

Special branch supported models

The following models are released on a special branch of FortiOS 5.4.6. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1165.

FGR-30D	is released on build 7686.
FGR-35D	is released on build 7686.
FGR-30D-A	is released on build 7686.
FG-30E-MI	is released on build 6406.
FG-30E-MN	is released on build 6406.
FWF-30E-MI	is released on build 6406.
FWF-30E-MN	is released on build 6406.
FWF-50E-2R	is released on build 7688.
FG-52E	is released on build 6401.
FG-60E	is released on build 6408.
FWF-60E	is released on build 6408.
FG-61E	is released on build 6408.
FWF-61E	is released on build 6408.
FG-80E	is released on build 6408.
FG-80E-POE	is released on build 6408.
FG-81E	is released on build 6408.
FG-81E-POE	is released on build 6408.
FG-90E	is released on build 6405.
FG-90E-POE	is released on build 6405.
FG-91E	is released on build 6405.
FWF-92D	is released on build 7687.
FG-100E	is released on build 6408.

FG-100EF	is released on build 6408.
FG-101E	is released on build 6408.
FG-140E	is released on build 6408.
FG-140E-POE	is released on build 6408.
FG-200E	is released on build 6402.
FG-201E	is released on build 6402.
FG-300E	is released on build 4075.
FG-301E	is released on build 4075.
FG-500E	is released on build 4075.
FG-501E	is released on build 4075.
FG-2000E	is released on build 6403.
FG-2500E	is released on build 6403.
FG-3960E	is released on build 6404.
FG-3980E	is released on build 6404.
FG-5001E	is released on build 6400.
FG-VM64-AZURE	is released on build 6399.
FG-VM64-AZUREONDEMAND	is released on build 6399.

What's new in FortiOS 5.4.6

For a detailed list of new features and enhancements that have been made in FortiOS 5.4.6, see the *What's New for FortiOS* 5.4.6 document available in the Fortinet Document Library.

Special Notices

Built-In Certificate

FortiGate and FortiWiFi D-series and above have a built in Fortinet_Factory certificate with an RSA 2048-bit key; and FortiOS supports DH group 14 for key-exchange.

Default log setting change

For FG-5000 blades, log disk is disabled by default. It can only be enabled via CLI. For all 2U & 3U models (FG-3600/FG-3700/FG-3800), log disk is also disabled by default. For all 1U models and desktop models that supports SATA disk, log disk is enabled by default.

Policy list display changes

To improve performance, FortiOS 5.4.6 implemented the following changes when displaying lists in *Policy & Objects*.

In *Policy & Objects* > *Addresses*:

- The *Address* | *Group* | *All* option at the top is removed and all addresses and groups are displayed in sections.
- Paging options at the bottom are removed.
- The group member count is moved to the *Details* column.

In *Policy & Objects* > *Policy* lists:

- The *Sequence* view and *Seq.#* column are removed.
- Custom sections (global-labels) are no longer supported.
- To start searching, press Enter, click the search button, or click outside the search box.
- Column filters are reset when you leave or reload the page.
- Section expand/collapse settings are reset when you leave or reload the page.

FortiAnalyzer support

In version 5.4, encrypting logs between FortiGate and FortiAnalyzer is handled via SSL encryption. The IPsec option is no longer available and users should reconfigure in GUI or CLI to select the SSL encryption option as needed.

Removed SSL/HTTPS/SMTPS/IMAPS/POP3S

SSL/HTTPS/SMTPS/IMAPS/POP3S options were removed from server-load-balance on low end models below FG-100D except FG-80C and FG-80CM.

FortiGate and FortiWiFi-92D hardware limitation

FortiOS 5.4.0 reported an issue with the FG-92D model in the *Special Notices > FG-92D High Availability in Interface Mode* section of the release notes. Those issues, which were related to the use of port 1 through 14, include:

- PPPoE failing, HA failing to form
- IPv6 packets being dropped
- FortiSwitch devices failing to be discovered
- Spanning tree loops may result depending on the network topology

FG-92D and FWF-92D do not support STP. These issues have been improved in FortiOS 5.4.1, but with some side effects with the introduction of a new command, which is enabled by default:

```
config system global
   set hw-switch-ether-filter <enable | disable>
```

When the command is enabled:

- ARP (0x0806), IPv4 (0x0800), and VLAN (0x8100) packets are allowed
- BPDUs are dropped and therefore no STP loop results
- PPPoE packets are dropped
- IPv6 packets are dropped
- FortiSwitch devices are not discovered
- HA may fail to form depending the network topology

When the command is disabled:

- All packet types are allowed, but depending on the network topology, an STP loop may result

FG-900D and FG-1000D

CAPWAP traffic will not offload if the ingress and egress traffic ports are on different NP6 chips. It will only offload if both ingress and egress ports belong to the same NP6 chip.

FG-3700DX

CAPWAP Tunnel over the GRE tunnel (CAPWAP + TP2 card) is not supported.

FortiGate units managed by FortiManager 5.0 or 5.2

Any FortiGate unit managed by FortiManager 5.0.0 or 5.2.0 may report installation failures on newly created VDOMs, or after a factory reset of the FortiGate unit even after a retrieve and re-import policy.

FortiClient support

Only FortiClient 5.4.1 and later is supported with FortiOS 5.4.1 and later. Upgrade managed FortiClients to 5.4.1 or later before upgrading FortiGate to 5.4.1 or later.

Consider the FortiClient license before upgrading. Full featured FortiClient 5.2 and 5.4 licenses will carry over into FortiOS 5.4.1 and later. Depending on your organization's needs, you might need to purchase a FortiClient EMS license for endpoint provisioning. Contact your sales representative for guidance on the appropriate licensing for your organization.

The perpetual FortiClient 5.0 license (including the 5.2 limited feature upgrade) will not carry over into FortiOS 5.4.1 and later. You need to purchase a new license for either FortiClient EMS or FortiGate. A license is compatible with 5.4.1 and later if the SKU begins with FC-10-C010.

FortiClient (Mac OS X) SSL VPN requirements

When using SSL VPN on Mac OS X 10.8, you must enable SSLv3 in FortiOS.

FortiGate-VM 5.4 for VMware ESXi

Upon upgrading to FortiOS 5.4.6, FortiGate-VM v5.4 for VMware ESXi (all models), no longer supports the VMXNET2 vNIC driver.

FortiClient profile changes

With introduction of the Cooperative Security Fabric in FortiOS, FortiClient profiles will be updated on FortiGate. FortiClient profiles and FortiGate are now primarily used for Endpoint Compliance, and FortiClient Enterprise Management Server (EMS) is now used for FortiClient deployment and provisioning.

In the FortiClient profile on FortiGate, when you set the *Non-Compliance Action* setting to *Auto-Update*, the FortiClient profile supports limited provisioning for FortiClient features related to compliance, such as AntiVirus, Web Filter, Vulnerability Scan, and Application Firewall. When you set the *Non-Compliance Action* setting to *Block* or *Warn*, you can also use FortiClient EMS to provision endpoints, if they require additional other features, such as VPN tunnels or other advanced options. For more information, see the *FortiOS Handbook – Security Profiles*.

When you upgrade to FortiOS 5.4.1 and later, the FortiClient provisioning capability will no longer be available in FortiClient profiles on FortiGate. FortiGate will be used for endpoint compliance and Cooperative Security Fabric integration, and FortiClient Enterprise Management Server (EMS) should be used for creating custom FortiClient installers as well as deploying and provisioning FortiClient on endpoints. For more information on licensing of EMS, contact your sales representative.

FortiPresence

FortiPresence users must change the FortiGate web administration TLS version in order to allow the connections on all versions of TLS. Use the following CLI command.

```
config system global
   set admin-https-ssl-versions tlsv1-0 tlsv1-1 tlsv1-2
end
```

Log disk usage

Users are able to toggle disk usage between Logging and WAN Optimization for single disk FortiGates.

To view a list of supported FortiGate models, refer to the FortiOS 5.4.0 Feature Platform Matrix.

SSL VPN setting page

The default server certificate has been changed to the `Fortinet_Factory` option. This excludes FortiGate-VMs which remain at the `self-signed` option. For details on importing a CA signed certificate, please see the How to purchase and import a signed SSL certificate document.

FG-30E-3G4G and FWF-30E-3G4G MODEM firmware upgrade

The 3G4G MODEM firmware on the FG-30E-3G4G and FWF-30E-3G4G models may require updating. Upgrade instructions and the MODEM firmware have been uploaded to the Fortinet Customer Service & Support site. Log in and go to *Download* > *Firmware*. In the *Select Product* list, select *FortiGate*, and click the *Download* tab. The upgrade instructions are in the following directory:

.../FortiGate/v5.00/5.4/Sierra-Wireless-3G4G-MODEM-Upgrade/

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

DLP, AV

In 5.2, Block page was sent to client with HTTP status code `200` by default. In 5.4 and later, Block page is sent to client with a clearer HTTP status code of `403 Forbidden`.

Using ssh-dss algorithm to log in to FortiGate

In version 5.4.5 and later, using `ssh-dss` algorithm to log in to FortiGate via SSH is no longer supported.

Upgrade Information

Upgrading to FortiOS 5.4.6

FortiOS version 5.4.6 officially supports upgrading from version 5.4.4 and later, and 5.2.10 and later.

When upgrading from a firmware version beyond those mentioned in the Release Notes, a recommended guide for navigating the upgrade path can be found on the Fortinet documentation site.

There is a separate version of the guide describing the safest upgrade path to the latest patch of each of the supported versions of the firmware. To upgrade to this build, go to FortiOS 5.4 Supported Upgrade Paths.

Upgrading to FortiOS 5.6.0

This only applies if you are upgrading to version 5.6.0. If you are upgrading to version 5.6.1 or later, you don't need to reconfigure IPsec settings.

If you have configured IPsec in version 5.4.6 and you upgrade to 5.6.0, you must reconfigure all IPsec phase1 `psksecret` settings after upgrading to 5.6.0 in order to establish an IPsec tunnel.

Cooperative Security Fabric upgrade

FortiOS 5.4.1 and later greatly increases the interoperability between other Fortinet products. This includes:

- FortiClient 5.4.1 and later
- FortiClient EMS 1.0.1 and later
- FortiAP 5.4.1 and later
- FortiSwitch 3.4.2 and later

The upgrade of the firmware for each product must be completed in a precise order so the network connectivity is maintained without the need of manual steps. Customers must read the following two documents prior to upgrading any product in their network:

- *Cooperative Security Fabric - Upgrade Guide*
- *FortiOS 5.4.x Upgrade Guide for Managed FortiSwitch Devices*

  This document is available in the Customer Support Firmware Images download directory for FortiSwitch 3.4.2.

FortiGate-VM 5.4 for VMware ESXi

Upon upgrading to FortiOS 5.4.6, FortiGate-VM v5.4 for VMware ESXi (all models), no longer supports the VMXNET2 vNIC driver.

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- VDOM parameters/settings
- admin user account
- session helpers
- system access profiles

When downgrading from 5.4 to 5.2, users will need to reformat the log disk.

Amazon AWS enhanced networking compatibility issue

Due to this new enhancement, there is a compatibility issue with older AWS VM versions. After downgrading a 5.4.1 or later image to an older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover the downgraded image.

Downgrading to older versions from 5.4.1 or later running the enhanced nic driver is not allowed. The following AWS instances are affected:

- C3
- C4
- R3
- I2
- M4
- D2

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiOS 5.4.6 support

The following table lists 5.4.6 product integration and support information:

Web Browsers	• Microsoft Edge 38 • Mozilla Firefox version 53 • Google Chrome version 58 • Apple Safari version 9.1 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 40 • Mozilla Firefox version 53 • Apple Safari version 10 (For Mac OS X) • Google Chrome version 58 Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	For the latest information, see the FortiManager and FortiOS Compatibility. You should upgrade your FortiManager prior to upgrading the FortiGate.
FortiAnalyzer	For the latest information, see the FortiAnalyzer and FortiOS Compatibility. You should upgrade your FortiAnalyzer prior to upgrading the FortiGate.
FortiClient Microsoft Windows and FortiClient Mac OS X	• 5.4.1 and later If FortiClient is being managed by a FortiGate, you must upgrade FortiClient before upgrading the FortiGate.
FortiClient iOS	• 5.4.1 and later
FortiClient Android and FortiClient VPN Android	• 5.4.0 and later

FortiAP	• 5.4.1 and later • 5.2.5 and later Before upgrading FortiAP units, verify that you are running the current recommended FortiAP version. To do this in the GUI, go to the *WiFi Controller > Managed Access Points > Managed FortiAP*. If your FortiAP is not running the recommended version, the *OS Version* column displays the message: *A recommended update is available*.
FortiAP-S	• 5.4.1 and later
FortiSwitch OS (FortiLink support)	• 3.5.0 and later
FortiController	• 5.2.0 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C • 5.0.3 and later Supported model: FCTL-5103B
FortiSandbox	• 2.1.0 and later • 1.4.0 and later

Fortinet Single Sign-On (FSSO)	• 5.0 build 0264 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2016 Server Edition
	  • Windows Server 2016 Datacenter
	  • Windows Server 2008 (32-bit and 64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Novell eDirectory 8.8
	• 4.3 build 0164 (contact Support for download)
	  • Windows Server 2003 R2 (32-bit and 64-bit)
	  • Windows Server 2008 (32-bit and 64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2012 Standard Edition
	  • Windows Server 2012 R2
	  • Novell eDirectory 8.8
	FSSO does not currently support IPv6.

FortiExplorer	• 2.6.0 and later. Some FortiGate models may be supported on specific FortiExplorer versions.

FortiExplorer iOS	• 1.0.6 and later Some FortiGate models may be supported on specific FortiExplorer iOS versions.
FortiExtender	• 3.0.0 • 2.0.2 and later
AV Engine	• 5.247
IPS Engine	• 3.438
Virtualization Environments	
Citrix	• XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Microsoft	• Hyper-V Server 2008 R2, 2012, 2012 R2, and 2016
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5
VM Series - SR-IOV	The following NIC chipset cards are supported: • Intel 82599 • Intel X540 • Intel X710/XL710

FortiGate-VM v5.4 for VMware ESXi (all models), no longer supports the VMXNET2 vNIC driver.

Language support

The following table lists language support information.

Language support

Language	GUI
English	✔
Chinese (Simplified)	✔
Chinese (Traditional)	✔
French	✔
Japanese	✔
Korean	✔
Portuguese (Brazil)	✔
Spanish (Spain)	✔

SSL VPN support

SSL VPN standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

Operating system and installers

Operating System	Installer
Linux CentOS 6.5 / 7 (32-bit & 64-bit) Linux Ubuntu 16.04	2333. Download from the Fortinet Developer Network https://fndn.fortinet.net.

Other operating systems may function correctly, but are not supported by Fortinet.

SSL VPN standalone client no longer supports the following operating systems:

- Microsoft Windows 7 (32-bit & 64-bit)
- Microsoft Windows 8 / 8.1 (32-bit & 64-bit)
- Microsoft Windows 10 (64-bit)
- Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit) Microsoft Windows 8 / 8.1 (32-bit & 64-bit)	Microsoft Internet Explorer version 11 Mozilla Firefox version 53 Google Chrome version 58
Microsoft Windows 10 (64-bit)	Microsoft Edge Microsoft Internet Explorer version 11 Mozilla Firefox version 53 Google Chrome version 58
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 53
Mac OS 10.11.1	Apple Safari version 9 Mozilla Firefox version 53 Google Chrome version 58
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

SSL VPN host compatibility list

It is recommended to verify the accuracy of the GUID for the software you are using for SSLVPN host check. The following Knowledge Base article at http://kb.fortinet.com/ describes how to identify the GUID for antivirus and firewall products: How to add non listed 3rd Party AntiVirus and Firewall product to the FortiGate SSL VPN Host check.

After verifying GUIDs, you can update GUIDs in FortiOS by using this command:

```
config vpn ssl web host-check-software
```

Following is an example of how to update the GUID for AVG Internet Security 2017 on Windows 7 and Windows 10 by using the FortiOS CLI.

The GUIDs in this example are only for AVG Internet Security 2017 on Windows 7 and Windows 10. The GUIDs might be different for other versions of the software and other operation systems.

To update GUIDs in FortiOS:

1. Use the `config vpn ssl web host-check-software` command to edit the `AVG-Internet-Security-AV` variable to set the following GUID for AVG Internet Security 2017: `4D41356F-32AD-7C42-C820-63775EE4F413`
2. Edit the `AVG-Internet-Security-FW` variable to set the following GUID: `757AB44A-78C2-7D1A-E37F-CA42A037B368`

Resolved Issues

The following issues have been fixed in version 5.4.6. For inquires about a particular bug, please contact Customer Service & Support.

AntiVirus

Bug ID	Description
300206	Proxy-AV POP3 44k throughput test constantly has aborted transactions with low stress level.
442328	Replacement message image fails to load.

DNS Filter

Bug ID	Description
402831	DNS Filter and Interface page botnet DB check should be updated.
420170	Skip the rating for Dynamic DNS update type queries.
422407	`dnsproxy` process runing high CPU causing degradation of DNS traffic.
438834	DNS Filter blocks access when rating error occurs, even with allow request on rating error enabled.

Firewall

Bug ID	Description
403514	Broadcast packets are not forwarded through VIP.
415035	Policy64 with VIP64 assigns incorrect SNAT IP 0.0.0.0.
421381	IPsec traffic matching NAT64 policy dropped by NP IPSEC0_IQUEUE.
423819	VIP64 does not work properly.
424558	Renaming onetime schedule causes policy activation.
435070	Full Cone NAT not working for WhatsApp Video and Voice Call.
435095	FortiOS ICMP replies or error messages are dropped when asymmetric routing is involved.

FortiGate-60D

Bug ID	Description
422755	`memory_tension_drop` increase even though memory usage is very low.

FortiGate-140E

Bug ID	Description
436126	RJ45 interfaces (wan1, wan2, port1-38) do not work when the speed setting is not set to auto.

FortiGate-5001D

Bug ID	Description
392883	SLBC slave blades with TP VDOMs cannot connect to FSSO Collector Agent.

FortiGate and FortiWifi E Series

Bug ID	Description
413699	In some FortiGate and FortiWifi E series models, the default *Inspection Mode* is flow-based instead of proxy-based. Affected models: FG-60E, FG-61E, FWF-60E, FWF-61E, FG-80E, FG-81E, FG-80E-POE, FG-81E-POE, FG-100E, FG-101E, FG-100EF, FG-140E, FG-140E-POE.

FortiSwitch

Bug ID	Description
435219	`cu_acd` causing memory leak leading to conserve mode.

FortiView

Bug ID	Description
390495	Cannot view websites in FortiView for 5 minutes, 1 hour, and 24 hours.

GUI

Bug ID	Description
367394	Colors configured for firewall address objects are not visible in firewall policy list.

Bug ID	Description
368070	Custom category is not referenced when used in a Web Filter profile.
372907	Reference page shows *no matching entries found* for VPN tunnel with special characters in tunnel name.
374521	Unable to *Revert* revisions in GUI.
378575	Disabled local rating categories are incorrectly added into new Web Filter profiles.
392500	In the GUI Interface Bandwidth widget, the speed keep jumping from real value to 0 bps.
397233	GUI improve visibility of hardware acceleration features and memory usage.
398397	Slowness in accessing *Policy and Address* page in GUI after upgrading from 5.2.2 to 5.4.1.
403146	Slow GUI *Policy* tab when there are more than 600 policies.
406486	*Permission denied* error is shown when changing AntiVirus configuration even when AntiVirus privilege is set to *Read-Write*.
408577	Admin and FortiClient profile cannot be displayed when language is Japanese.
409100	Edit admin/user, enable FortiToken mobile, click send activation email before saving would send empty activation code.
411415	Update FortiOS API to remove IPS sessions in parallel with firewall sessions.
421263	Multiple wildcard login accounts gives wrong guest account provisioning when *Post-login-banner* is enabled.
439160	Address object references are not displayed.

HA

Bug ID	Description
389861	SNMP query for `fgHaStatsSyncStatus` on slave unit reports master as `unsynchronized- "0"`.
392677	The HA widget shows the slave status as not synchronized when the status is synchronized.
412652	Unexpected behavior occurs when one cluster unit has a monitored port down and the other cluster unit has ping server issues.
421639	HA kernel routes are not flushed after failover, when cluster learns a high number of routes.
423144	Reliable syslog using dedicated HA management interface doesn't work.

Bug ID	Description
437390	HA failover triggered before `pingserver-failover-threshold` is reached.
438197	PPPoE connection is disrupted by HA failover/failback.
442085	After HA failover, the new master unit uses an OSPF MD5 authentication encryption sequence that is lower than the previous sequence number.
442663	No NTP sync and feature license invalid at backup device in FGSP cluster.

IPS

Bug ID	Description
422666	New mechanism to load IPS/App rules into CMDB to avoid FortiGate bootup failure or lockup.
434478	Information incorrect in `diag test app ipsmonitor 13`.
439245	When the firewall policy was applied by FortiManager, a crash log of the IPS engine occurred.
445174	IPS engine crash on some models causes reboot.
445900	SSL negotiation not completed when IPS and SSL Inspection profiles are present.

IPsec VPN

Bug ID	Description
396953	“Encapsulation GRE” (GRE over IPsec) does not allow self-originated traffic to enter the tunnel.
401847	Half of IPsec tunnels traffic lost 26 minutes after power on a spare 1500D.
416102	Traffic over IPsec VPN getting dropped after 2 pings when it is getting offloaded to NPU.
416950	NP6 stop process traffic through IPsec tunnel.

Logging & Report

Bug ID	Description
420147	Getting *Error connecting to FortiCloud* message when trying to access FortiCloud Reports in GUI.
445522	In *Local report - Web Usage* section, *Top users by bandwidth* seems to show the download as upload.

Router

Bug ID	Description
424381	Random TCP sessions get stuck or time out.

Spam

Bug ID	Description
410420	Spam emails are exempted if they are sent in one session.
416790	`(no.x pattern matched)` is not logged when bwl matches envelop MAIL FROM.

SSL VPN

Bug ID	Description
375137	SSL VPN bookmarks may be accessible after accessing more than ten bookmarks in web mode.
380974	SSL VPN sometimes gets key conflict when loading system provided keys.
401807	SSL VPN web mode for VNC could not launch pop up menu with F8.
412456	SSL VPN realm should be kept in the idle timeout redirected URL.
412850	SSL VPN Portal redirect not working. Fails with a Javascript error.
421261	Access to websites via Webbase SSL VPN returns empty page after browsing for some time.
448852	OTP for RSA Server are truncated if they are longer than eight digits.

System

Bug ID	Description
383624	Sending multicast traffic across NP6 inter-VDOM link may cause interfaces to stop sending/receiving.
392436	Slow throughput using 10G interfaces.
392655	Conserve mode - 4096 SLAB leak suspected.
393006	NPU offloading causes issues with Arista.
397266	Disable unnecessary FGT queries and RSS feeds.

Bug ID	Description
401360	LDAP search and group queries do not work.
407383	LACP will not negotiate on 100D ports 15 and 16 using FG-TRAN-SX.
408977	802.1AX L4 algorithm and NP4 do not distribute UDP evenly on egress LAG bundle.
415353	Telnet connection timing out with IPsec through MPLS when offloading is enabled.
415555	IPv6 `ipv6-neighbor-cache` configuration doesn't survive after a reboot or flush command.
415910	CPU cores utilization shows 0% while handling CPS.
416678	FG101E/100E has reports of firewall lockups in production.
420150	NTPv3 with authentication enabled fails with error `receive: authentication failed`.
421714	Merge kxp D state fix into 5.4.6.
423375	Some configurations are missing in the output of `show full-configuration`.
424213	Cluster Virtual MAC address changed to Physical port MAC address when Ports are assigned on MGMT-VDOM.
434480	Admin user session does not time out.
436211	Kernel conserve mode occurs due to memory leak.
437589	Slow throughput on 1000D between 10G and 1G interfaces.
437925	FWF-81CM `dnsproxy` daemon has high memory usage.
438088	U-Turn traffic in Transparent mode VDOM does not work anymore.
438205	Packets in reply direction get dropped if ingress interface is not the same as egress in original direction.
438405	HRX/PKTCHK Drops over NP6 with 1.5 Gbps.
439115	IP-to-IP-Tunnel does not forward packets after rebooting.
439469	Dropped packets only on the LACP Interface but not on the physicals that is part of the LAG.
439897	Virtual wire pair on asymmetric environment.
440412	Added SNMP trap for per-CPU usage.

Bug ID	Description
440923	The FortiGate interface DHCP client does not work properly in some situations.
441532	Suggest to add SNMP/CLI monitoring capabilities of NP6 session table.

Upgrade

Bug ID	Description
273973	When upgrading from 5.2 to 5.4, the Central NAT feature cannot be upgraded. After the upgrade, reconfigure the Central NAT feature. Please see the configuration examples in the FortiOS Handbook available in the Fortinet Document Library.
404089	Uninterruptible upgrade failed because routes are not yet synced on new master.

User and FSSO

Bug ID	Description
378085	User authentication timeout max. setting change.
378207	`authd` process running high CPU when only RSSO logging is configured.
412487	RSSO Endpoint Storage limits the number of characters to 48.
437204	`authd` sends malformed NTLM TYPE2 to browser and breaks NTLM authentication.
438758	A CRL update on the FortiGate does not trigger an auto-update to the FortiManager.

VM

Bug ID	Description
424452	SNMP traps not being sent when interface is down.
441294	The network bandwidth show a zero value.

VoIP

Bug ID	Description
423437	SIP ALG does not translate all MSRP SEND messages if more than one SEND message is contained within a single packet.

Web Filter

Bug ID	Description
409110	Web page override login page loads slowly.
420967	Proxy AV + Proxy WF + SSL Certificate Inspection (Inspect All Ports) results in HTTPS traffic bypassing Web Filter.
423020	Regex value changes in the URL filter.
435258	Send Fin/Ack to the client during HTTP POST request.
436354	Replace Message Group *Web Filter Block Override* page not working.

WebProxy

Bug ID	Description
412404	Cannot access some HTTPS websites due to `ERR_SSL_PROTOCOL_ERROR`.
415385	Explicit FTP proxy issue on zero file size transfers.
416208	WAD Dispatcher reached FD limit with large number of CLOSE_WAIT sockets, some workers entered "D" state.
417001	Explicit HTTP proxy drops HTTPS connections on Web Filter rating failures.
417491	WAD crashed when handling FTP over HTTP traffic.
418193	Some HTTPS sites show *Secure Connection Failed* with flow-based Web Filter (static URL filter only) and SSL certificate inspection.
423077	WAD crashed after upgrading from 5.2.10 to 5.4.4 GA release.
434787	FortiGate deep inspection is causing *nonconforming extension* certificate error on MAC, Android, and Chromebook devices.
435283	`block-page-status-code` doesn't work for HTTP status code of the DLP replacement message.

WiFi

Bug ID	Description
364688	Packet loss when offloading CAPWAP traffic.
434991	WTP tablesize limitation cause WTP entry to be lost after upgrade from 5.4.4 to 5.4.5. Affected models: FG-30D, FG-30D-POE, FG-30E, FWF-30D, FWF-30D-POE, FWF-30E.

Bug ID	Description
437949	Split tunnel enhancement: `set split-tunneling-acl-path [tunnel | local].`

Common Vulnerabilities and Exposures

Bug ID	CVE references
405122	FortiOS 5.4.6 is no longer vulnerable to the following CVE Reference: • 2017-3732 • 2017-7055 Visit https://fortiguard.com/psirt for more information.
415416	FortiOS 5.4.6 is no longer vulnerable to the following CVE Reference: • 2017-7733 Visit https://fortiguard.com/psirt for more information.
416322	FortiOS 5.4.6 is no longer vulnerable to the following CVE Reference: • 2017-2636 Visit https://fortiguard.com/psirt for more information.
422133	FortiOS 5.4.6 is no longer vulnerable to the following CVE Reference: • 2009-3555 Visit https://fortiguard.com/psirt for more information.
440744	FortiOS 5.4.6 is no longer vulnerable to the following CVE Reference: • 2017-7739 Visit https://fortiguard.com/psirt for more information.
442365	FortiOS 5.4.6 is no longer vulnerable to the following CVE Reference: • 2017-7738 Visit https://fortiguard.com/psirt for more information.
446892	FortiOS 5.4.6 is no longer vulnerable to the following CVE Reference: • 2017-13077 • 2017-13078 • 2017-13079 • 2017-13080 • 2017-13081 • 2017-13082 Visit https://fortiguard.com/psirt for more information.
449257	FortiOS 5.4.6 is no longer vulnerable to the following CVE Reference: • 2017-14182 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in version 5.4.6. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

AntiVirus

Bug ID	Description
374969	FortiSandbox FortiView may not correctly parse the FSA v2.21 tracer file(.json).

Endpoint Control

Bug ID	Description
374855	Third party compliance may not be reported if FortiClient has no AV feature.
375149	FortiGate does not auto update AV signature version while Endpoint Control (`fortiheartbeat`) is enabled but no AV profile is used.
391537	Buffer size is too small when sending large vulnerability list to FortiGate.

Firewall

Bug ID	Description
364589	LB VIP slow access when cookie persistence is enabled.

FortiGate-3815D

Bug ID	Description
385860	FortiGate-3815D does not support 1 GE SFP transceivers.

FortiRugged-60D

Bug ID	Description
375246	`invalid hbdev dmz` may be received if the default `hbdev` is used.

FortiSwitch-Controller/FortiLink

Bug ID	Description
304199	Using HA with FortiLink can encounter traffic loss during failover.
357360	DHCP snooping may not work on IPv6.
369099	FortiSwitch authorizes successfully but fails to pass traffic until you reboot FortiSwitch.

FortiView

Bug ID	Description
368644	*Physical Topology: Physical Connection* of stacked FortiSwitch may be incorrect.
372350	*Threat view: Threat Type and Event* information is missing in the last level of the threat view.
373142	*Threat: Filter* result may not be correct when adding a filter on a threat and threat type on the first level.
375187	Using realtime auto update may increase chrome browser memory usage.

GUI

Bug ID	Description
289297	Threat map may not be fully displayed when screen resolution is not big enough.
297832	Administrator with read-write permission for *Firewall Configuration* is not able to read or write firewall policies.
355388	The *Select* window for remote server in remote user group may not work as expected.
365223	In Security Fabric topology, a downstream FortiGate may be shown twice when it uses hardware switch to connect upstream.
365317	Unable to add new AD group in second FSSO local polling agent.
365378	You may not be able to assign `ha-mgmt-interface` IP address in the same subnet as another port from the GUI.
368069	Cannot select `wan-load-balance` or members for incoming interface of IPsec tunnel.
369155	There is no `Archived Data` tab for email attachment in the DLP log detail page.
372908	The interface tooltip keeps loading the VLAN interface when its physical interface is in another VDOM.

Bug ID	Description
372943	Explicit proxy policy may show a blank for default authentication method.
373363	Multicast policy interface may list the `wan-load-balance interface`.
373546	Only 50 security logs may be displayed in the *Log Details* pane when more than 50 are triggered.
374081	`wan-load-balance interface` may be shown in the address associated interface list.
374162	GUI may show the modem status as `Active` in the `Monitor` page after setting the modem to disable.
374224	The *Ominiselect* widget and *Tooltip* keep loading when clicking a newly created object in the *Firewall Policy* page.
374320	Editing a user from the *Policy* list page may redirect to an empty user edit page.
374322	*Interfaces* page may display the wrong MAC Address for the hardware switch.
374363	Selecting *Connect to CLI* from managed FAP context menu may not connect to FortiAP.
374373	*Policy View: Filter* bar may display the IPv4 policy name for the IPv6 policy.
374397	Should only list `any` as destination interface when creating an explicit proxy in the TP VDOM.
374525	When activating the *FortiCloud/Register-FortiGate*, clicking *OK* may not work the first time.
375036	The *Archived Data* in the *Sniffer Traffic* log may not display detailed content and download.
375227	You may be able to open the dropdown box and add new profiles even though errors occur when editing a *Firewall Policy* page.
375259	`Addrgrp` editing page receives a `js` error if `addrgrp` contains another group object.
375346	You may not be able to download the application control packet capture from the forward traffic log.
375369	May not be able to change IPsec `manualkey config` in GUI.
375383	The *Policy* list page may receive a `js` error when clicking the search box if the policy includes `wan-load-balance interface`.
379050	User Definition intermittently not showing assigned token.
421423	Cannot download certificate in *Security Profiles* > *SSL/SSH Inspection*. Workaround: Go to *System* > *Certificates* to download.

Bug ID	Description
453751	In IE11, the *Policy and Address* page keeps reloading when there are many entries.
454259	The *Policy* list page does not display tooltips for policy comments.
456566	In firewall policy list, need to add support for custom sections.

HA

Bug ID	Description
399115	ID for the new policy (when using edit 0) is different on master and on slave unit.

IPsec

Bug ID	Description
393958	Shellshock attack succeeds when FGT is configured with `server-cert-mode replace` and an attacker uses `rsa_3des_sha`.
435124	Cannot establish IPsec phase1 tunnel after upgrading from version 5.4.5 to 5.6.0. Workaround: After upgrading to 5.6.0, reconfigure all IPsec phase1 `psksecret` settings.
439923	IKE static tunnels using `set peertype one` may fail to negotiate.

SSL VPN

Bug ID	Description
303661	The Start Tunnel feature may have been removed.
304528	SSL VPN Web Mode PKI user might immediately log back in even after logging out.
374644	SSL VPN tunnel mode Fortinet bar may not be displayed.
382223	SMB/CIFS bookmark in SSL VPN portal doesn't work with DFS Microsoft file server error "Invalid HTTP request".
404863	In SSL VPN Web Mode, clicking new bookmark gets error `Internal: invalid parameter`.

System

Bug ID	Description
287612	Span function of software switch may not work on FortiGate-51E/FortiGate-30E.

Bug ID	Description
290708	`nturbo` may not support CAPWAP traffic.
295292	If `private-data-encryption` is enabled, when restoring config to a FortiGate, the FortiGate may not prompt the user to enter the key.
304199	FortiLink traffic is lost in HA mode.
371320	`show system interface` may not show the *Port* list in sequential order.
372717	Option `admin-https-banned-cipher` in `sys global` may not work as expected.
392960	FOS support for V4 BIOS.
445383	Traffic cannot go through LACP static mode interface with NP6 offload enabled.

Upgrade

Bug ID	Description
289491	When upgrading from 5.2.x to 5.4.0, port-pair configuration may be lost if the `port-pair` name exceeds 12 characters.

Visibility

Bug ID	Description
374138	FortiGate device with VIP configured may be put under Router/NAT devices because of an address change.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open Source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.

FORTINET®

High Performance Network Security